



Polycom[®] RealPresence[®] Access Director[™] System

Polycom announces the release of the Polycom RealPresence Access Director system, version 3.1.1. This document provides the latest information about this release.

Contents

- [New Features in Version 3.1.1](#) on page 1
- [Overview of the Polycom RealPresence Access Director System](#) on page 2
- [Installation and Upgrades](#) on page 4
- [Software Version History](#) on page 5
- [Documentation](#) on page 6
- [Products Tested with this Release](#) on page 7
- [Resolved Issues](#) on page 8
- [Known Issues](#) on page 9
- [Where to Get the Latest Information](#) on page 10

New Features in Version 3.1.1

Version 3.1.1 of the RealPresence Access Director system supports the following Cisco[®] endpoints (formerly TANDBERG[®]):

- Cisco C20 Codec
- Cisco EX90 Desktop System
- Cisco 1700 MXP Desktop System

Interoperability with Cisco Endpoints

The following limitations and interoperability issues may occur when using Cisco endpoints:

- Cisco C20 Codecs cannot use the far-end camera control function in VMR conferences.

- When a Cisco C20 Codec receives a SIP 401 message, it cannot send an authorized name and password in the re-INVITE message.
- Cisco 1700 MXP Desktop Systems cannot use the far-end camera control function.
- Cisco C20 Codecs, Cisco EX90 Desktop Systems, and Cisco 1700 MXP Desktop Systems cannot support content keep alive messages during an H.323 trusted B2B call and the Cisco endpoint user cannot see the other enterprise user's content.
- Cisco 1700 MXP Desktop Systems cannot support BFCP channel keep alive messages and the Cisco endpoint user cannot see content shared by other endpoints.

Overview of the Polycom RealPresence Access Director System

The RealPresence Access Director system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP and H.323 calls from registered users, guests, and federated enterprises or divisions from both AVC and SVC endpoints. The system provides secure communication between remote users and offices, and among guest users and organizations outside of the client's enterprise network.

The RealPresence Access Director system provides the following key services:

SIP Back-to-Back User Agent

The RealPresence Access Director system serves as a SIP back-to-back user agent (B2BUA) and operates between both end points of a SIP video call session. When a SIP call takes place, the RealPresence Access Director system divides the communication channel into two call legs and mediates all SIP signaling between both ends of the call, from call establishment to termination.

The RealPresence Access Director system SIP B2BUA supports the following call scenarios:

- SIP remote users with both AVC and SVC endpoints
- SIP guest users with both AVC and SVC endpoints

H.323 Signaling Proxy

- H.323 remote users with H.460 endpoints
- H.323 guest users
- H.323 enterprise-to-enterprise neighbored calling

Media Relay

- RTP and SRTP pass through

Access Proxy

- Management, RealPresence CloudAXIS Suite, and other HTTPS application servers

- Presence (XMPP)
- Directory (LDAP)
- Passthrough reverse proxy to servers not supported by other access proxy protocols.
- HTTP tunnel (SIP signaling and media relay for SIP guest call HTTP requests from RealPresence CloudAXIS Suite clients)

Security

- Deployable behind outside firewalls that use Network Address Translation (NAT)
- Secured communications (TLS and certificates)
- Secure management (Syslog, LDAP authentication, and role-based access control)
- Server-side authentication
- Server-side session management
- Robust SIP TLS cipher
- OS hardening

Operating System

- CentOS 5.7 (2.6.18-274.el5)

Performance

- 1,000 simultaneous calls
- 600-700 MB throughput
- 5,000 concurrent registrations
- 20 call attempts per second for SIP calls
- 10 call attempts per second for H.323 calls

Endpoints (AVC and SVC)

- HDX systems
- RealPresence Group Series 300/500
- RealPresence Mobile
- RealPresence Desktop
- RealPresence CloudAXIS Suite
- Cisco C20 Codec, EX90 Desktop System, 1700 MXP Desktop System (AVC only)

Installation and Upgrades

Installation of new RealPresence Access Director systems is managed through Polycom Global Services. For more information, please contact your Polycom representative.



Visit the Polycom Global Services (<http://support.polycom.com>) to verify that you have the latest software release and release information for the product.

System Upgrades

RealPresence Access Director systems running version 3.1 of the software can be upgraded to version 3.1.1 from the Maintenance > Software Upgrade page of the system's management interface. Follow the instructions in the online help for the Software Upgrade page to upload and install the upgrade package (.bin file).

Version 3.1.1 does not require a new license activation key.

If your system is not currently at version 3.1, you must perform interim upgrades before upgrading to version 3.1.1. See the Release Notes for each version of the RealPresence Access Director system to view specific upgrade instructions.

The following table describes the interim upgrade scenarios:

Table: System Upgrade Scenarios

Starting RealPresence Access Director System Version	Upgrade to
2.0.3 or 2.0.4	2.1
2.1	2.1.1
2.1.1	3.0
3.0	3.1
3.1	3.1.1

See the *Polycom RealPresence Access Director System Administrators Guide* and online help for upgrading and licensing procedures.

Software Version History

The following table lists system software versions for each release of the RealPresence Access Director system.

Table: Software Version History

Version	System	Release Date	Features
3.1.1	CentOS 5.7 Postgres 9.1 Java 7u21	April 2014	<ul style="list-style-type: none"> Support for Cisco endpoints
v3.1	CentOS 5.7 Postgres 9.1 Java 7u21	January 2014	<ul style="list-style-type: none"> SIP open business-to-business (B2B) calling, enabling calls to and from external SIP endpoints that are not registered or are not members of a federated enterprise or division. HTTP tunnel reverse proxy that provides firewall traversal for Polycom® RealPresence® CloudAXIS™ Suite clients making SIP guest calls to video conferences Increased flexibility of Access proxy services to support multiple reverse proxy configurations License key to enable strong encryption of the tunnel between the tunnel server and tunnel client in a two-box tunnel deployment. Support for the LDAP v3 extension StartTLS Support for Polycom® CMA® Desktop Systems
v3.0	CentOS 5.7 Postgres 9.1 Java 7u21	August 2013	<ul style="list-style-type: none"> Support for split interfaces for SIP and H.323 signaling traffic Tunnel deployment of two RealPresence Access Director Systems Support of H.460 endpoints Support of default destination alias for H.323 guest users Access control lists Call history and registration history Port ranges TCP reverse proxy for Polycom® RealPresence® CloudAXIS™ Suite clients Interoperability with Cisco VCS Expressway™ Enhanced security features
v2.1.1	CentOS 5.7 Postgres 9.1 Java 6u30	June 2013	<ul style="list-style-type: none"> Resolved some known issues

Table: Software Version History

Version	System	Release Date	Features
v2.1	CentOS 5.7 Postgres 9.1 Java 6u30	March 2013	<ul style="list-style-type: none"> • Support for SNMP v2c and v3 for monitoring system status • Static route configuration • H.323 guest policy to limit destinations for inbound H.323 calls from the Internet • Support of both SVC and AVC endpoints for calls between federated enterprises
v2.0.4	CentOS 5.7 Postgres 9.1 Java 6u30	January 2013	<ul style="list-style-type: none"> • Support for additional Polycom® RealPresence® products, including Content Sharing Suite, Collaboration Server 800s, Virtual Edition, and Group Series 300/500 • User interface updates • SIP and H.323 call disposition descriptions
v2.0	CentOS 5.7 Postgres 9.1 Java 6u30	December 2012	<ul style="list-style-type: none"> • SIP Back-to-Back User Agent (B2BUA) • H.323 signaling proxy for guest users and enterprise-to-enterprise federated calling • Media relay, including RTP and SRTP passthrough and SVC support for SIP remote users • Access proxy for management, presence, and directory traffic • DMZ deployment • Support for managed endpoints (Polycom HDX systems, RealPresence Mobile, RealPresence Desktop)

Documentation

For additional installation and deployment information, refer to the following documents:

- *Polycom RealPresence Access Director System Getting Started Guide or Polycom RealPresence Access Director System Getting Started Guide, Virtual Edition*
- *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*
- *Polycom RealPresence Access Director System Administrator's Guide*

Products Tested with this Release

Polycom RealPresence Access Director systems are tested extensively with a wide range of products. The following table lists the products that have been tested for compatibility with this release. The table does not include a complete inventory of compatible systems.



Polycom recommends that you upgrade all of your Polycom systems with the latest software versions. Any compatibility issues may already have been addressed by software updates. Go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html to find the Polycom Current Interoperability Matrix.

Product	Version
NAT, Firewall, Session Border Controllers	
Polycom RealPresence Access Director	3.1.1
Polycom Video Border Proxy (VBP) 5300E	11.2.16
Acme Packet® Net-Net 3820	SCX6.3.0 MR-2 GA (Build 385)
Management Systems and Recorders	
Polycom RealPresence Resource Manager	8.0 8.1
Polycom Converged Management Application Desktop	5.2.5
Polycom RSS 4000	8.5
Polycom RealPresence Content Sharing Suite	1.2.0
Microsoft Active Directory	
Gatekeepers, Gateways, and MCUs	
Polycom RealPresence Collaboration Server 1500, 2000, and 4000	8.1 8.3
Polycom RealPresence Collaboration Server 800s, Virtual Edition	8.1
Polycom RealPresence Distributed Media Application (DMA) 7000	6.0.3 6.0.4
Endpoints	
Polycom HDX 7000, 8000, and 9000 series	3.1.0 3.1.2
Polycom RealPresence Mobile	3.0 3.1
Polycom RealPresence Desktop	3.0 3.1

Product	Version
Polycom RealPresence Group Series 300/500	4.1.2 4.1.3
Cisco C20 Codec	TC6.2.1
Cisco EX90 Desktop System	TC6.2.1
Cisco 1700 MXP Desktop System	F9.3.1
Polycom Solution	
Polycom RealPresence CloudAXIS Suite	1.4.0

Resolved Issues

The following table lists the resolved issues in the version 3.1.1 release of the RealPresence Access Director system.

Issue ID	Description
EDGE-991	If an open SIP TLS connection from one RealPresence Access Director system to a second RealPresence Access Director system fails because the certificate is not verified, the first RealPresence Access Director system does not automatically try to connect to the second system using TCP.
EDGE-1024	In a two-system tunnel configuration, the tunnel server does not forward media for calls from a Polycom RealPresence Collaboration Server to an endpoint if Diffsev is enabled on the RealPresence Collaboration Server.
EDGE-1049	A Polycom RealPresence Group Series system endpoint does not receive video in calls made from Cisco MXP1700 endpoints through the RealPresence Access Director system.
EDGE-1054	An H.323 trunk B2B call fails if the call rate is not set to 512 Kbps.
EDGE-1065	If a RealPresence Access Director system has a SIP enterprise federation with a Cisco VCS system, inbound and outbound RTP traffic that should be routed through the RealPresence Access Director system is instead routed through the Cisco VCS system.
EDGE-1077	Audio and video fails on a connected call between a RealPresence Group Series endpoint and a Polycom HDX series guest user because the RealPresence Access Director system does not assign a port for the 200 OK message from the HDX series guest endpoint.

Known Issues

The following table lists the known issues of the RealPresence Access Director system, version 3.1.1, and of other products that affect use of the RealPresence Access Director system.

Category	Issue ID	Description	Workaround
Certificates	EDGE-915	When Online Certificate Status Protocol (OCSP) is enabled in the RealPresence Access Director system, OCSP does not check the server certificate unless mutual TLS for SIP signaling is configured between an endpoint and the RealPresence Access Director system.	
Certificates	EDGE-931	When creating a certificate signing request, up to 20 Subject Alternative Names (SANs) can be specified. If a SAN entry is entered and then deleted, leaving a blank line in the SAN list, the list of SANs does not update after clicking OK.	
User Interface	EDGE-937	In Admin > SNMP Settings, the Local engine ID field is blank.	
Active Call	EDGE-1060	During an H.323 call from a Cisco EX90 Desktop System to a RealPresence Desktop client, the Cisco EX90 Desktop System user can view content shared by the RealPresence Desktop client. However, the Diagnostics > Active Call page in the RealPresence Access Director system user interface does not display the port assigned to the content traffic.	
Polycom® CMA® Desktop Note: This is a CMA Desktop issue and not a RealPresence Access Director system issue.	CMAD-10551	CMA Desktop systems located inside enterprise networks with certain restrictive firewall rules cannot view content shared by a remote CMA Desktop user when the content is routed through the RealPresence Access Director system.	

Category	Issue ID	Description	Workaround
<p>Polycom® RealPresence® Group Series 300/500 endpoints</p> <p>Note: This is a Group Series issue and not a RealPresence Access Director system issue.</p>	EDGE-489	<p>When remotely upgrading a RealPresence Group Series 300/500 endpoint through the RealPresence Access Director system, the upgrade fails. The RealPresence Group Series 300/500 endpoints use the HTTP protocol to upgrade. For secure border management, the RealPresence Access Director system supports the HTTPS protocol. When RealPresence Group Series 300/500 endpoints support HTTPS upgrades, this issue will be resolved.</p>	
<p>Cisco VCS Expressway</p> <p>Note This is a Cisco VCS Expressway issue and not a RealPresence Access Director system issue.</p>	EDGE-749	<p>A Cisco VCS Expressway call from an endpoint in an enterprise using Cisco VCS Control plus VCS Expressway to an endpoint in an enterprise using the RealPresence Access Director system and a RealPresence DMA system fails if SIP authentication is enabled in the DMA system. Cisco VCS Expressway currently does not support SIP enterprise-to-enterprise calls.</p>	

Where to Get the Latest Information

To view the latest Polycom RealPresence Access Director system product documentation, visit the Support page of the Polycom website at <http://support.polycom.com>.

Trademark Information



POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.



Java is a registered trademark of Oracle America, Inc., and/or its affiliates.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

© 2012-2014 Polycom, Inc. All rights reserved.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.